

## Exhibit 2



# Combating Trafficking in Counterfeit and Pirated Goods

Report to the President of the United States

*January 24, 2020*



Homeland  
Security

*Office of Strategy, Policy & Plans*

## Table of Contents

Table of Contents .....	2
1. Executive Summary .....	4
2. Introduction.....	7
3. Overview of Counterfeit and Pirated Goods Trafficking .....	10
4. Health and Safety, Economic, and National Security Risks .....	16
5. How E-Commerce Facilitates Counterfeit Trafficking.....	20
6. Private Sector Outreach and Public Comment.....	24
7. Immediate Action by DHS and Recommendations for the USG .....	26
8. Private Sector Best Practices .....	34
9. Conclusions.....	41
10. Appendix A: The IPR Center.....	42
11. Appendix B: Ongoing CBP Activities to Combat Counterfeit Trafficking.....	44
12. Appendix C: Homeland Security Investigations.....	47
13. Appendix D: U.S. Government Efforts.....	49
14. Appendix E: Global Initiatives .....	52
15. References.....	54

## Foreword/Message from the Acting Secretary of Homeland Security

The rapid growth of e-commerce has revolutionized the way goods are bought and sold, allowing for counterfeit and pirated goods to flood our borders and penetrate our communities and homes. Illicit goods trafficked to American consumers by e-commerce platforms and online third-party marketplaces threaten public health and safety, as well as national security. This illicit activity impacts American innovation and erodes the competitiveness of U.S. manufacturers and workers.

Consumers must be confident in the safety, quality, and authenticity of the products they purchase online. DHS is committed to combating counterfeiters and pirates with the help of our U.S. Government partners and private sector stakeholders - who are critical to helping secure supply chains to stem the tide of counterfeit and pirated goods.



“Combating Trafficking in Counterfeit and Pirated Goods,” has been prepared by the U.S. Department of Homeland Security’s Office of Strategy, Policy, and Plans. The report uses available data, substantial public input, and other information to develop a deeper understanding of how e-commerce platforms, online third-party marketplaces, and other third-party intermediaries facilitate the importation and sale of massive amounts of counterfeit and pirated goods. The report identifies appropriate administrative, statutory, regulatory, and other actions, including enhanced enforcement measures, modernization of legal and liability frameworks, and best practices for private sector stakeholders. These strong actions can be implemented swiftly to substantially reduce trafficking in counterfeit and pirated goods while promoting a safer America.

This report was prepared pursuant to President Donald J. Trump’s April 3, 2019, *Memorandum on Combating Trafficking in Counterfeit and Pirated Goods*. The President’s historic memorandum provides a much warranted and long overdue call to action in the U.S. Government’s fight against a massive form of illicit trade that is inflicting significant harm on American consumers and businesses. This illicit trade must be stopped in its tracks.

This report was prepared in coordination with the Secretaries of Commerce and State, the Attorney General, the Office of Management and Budget, the Intellectual Property Enforcement Coordinator, the United States Trade Representative, the Assistant to the President for Economic Policy, the Assistant to the President for Trade and Manufacturing Policy, and with other partners in the U.S. Government. The report also benefitted from extensive engagement with the private sector.

Sincerely,

Chad Wolf  
Acting Secretary,  
U.S. Department of Homeland Security

## 1. Executive Summary

The President’s April 3, 2019, *Memorandum on Combating Trafficking in Counterfeit and Pirated Goods* calls prompt attention to illicit trade that erodes U.S. economic competitiveness and catalyzes compounding threats to national security and public safety.

Counterfeiting is no longer confined to street-corners and flea markets. The problem has intensified to staggering levels, as shown by a recent Organisation for Economic Cooperation and Development (OECD) report, which details a 154 percent increase in counterfeits traded internationally — from \$200 billion in 2005 to \$509 billion in 2016. Similar information collected by the U.S. Department of Homeland Security (DHS) between 2000 and 2018 shows that seizures of infringing goods at U.S. borders have increased 10-fold, from 3,244 seizures per year to 33,810.

Relevant to the President’s inquiry into the linkages between e-commerce and counterfeiting, OECD reports that “E-commerce platforms represent ideal storefronts for counterfeits and provide powerful platform[s] for counterfeiters and pirates to engage large numbers of potential consumers.”<sup>1</sup> Similarly, the U.S. Government Accountability Office (GAO) found that e-commerce has contributed to a shift in the sale of counterfeit goods in the United States, with consumers increasingly purchasing goods online and counterfeiters producing a wider variety of goods that may be sold on websites alongside authentic products.

Respondents to the July 10, 2019, Federal Register Notice issued by the Department of Commerce echoed these observations.<sup>2</sup> Perhaps most notably, the International Anti-Counterfeiting Coalition (IACC) reports that the trafficking of counterfeit and pirated goods in e-commerce is a top priority for every sector of its membership — comprised of more than 200 corporations, including many of the world’s best-known brands in the apparel, automotive, electronics, entertainment, luxury goods, pharmaceutical, personal care and software sectors. The IACC submission goes on to say:

*Across every sector of the IACC’s membership, the need to address the trafficking of counterfeit and pirated goods in e-commerce has been cited as a top priority. The vast amounts of resources our members must dedicate to ensuring the safety and vitality of the online marketplace, bears out the truth of the issue highlighted by Peter Navarro, Assistant to the President for Trade and Manufacturing Policy, in his April 3, 2019 Op-Ed piece in The Wall Street Journal - that the sale of counterfeit brand-name goods presents a pervasive and ever-growing threat in the online space. One IACC member reported making*

---

<sup>1</sup> OECD (2018), *Governance Frameworks to Counter Illicit Trade*, Illicit Trade, OECD Publishing, Paris, <https://doi.org/10.1787/9789264291652-en>.

<sup>2</sup> Under Federal Register Notice (84 FR 32861), the Department of Commerce sought “comments from intellectual property rights holders, online third-party marketplaces and other third-party intermediaries, and other private-sector stakeholders on the state of counterfeit and pirated goods trafficking through online third-party marketplaces and recommendations for curbing the trafficking in such counterfeit and pirated goods.”

*hundreds of investigative online test purchases over the past year, with a nearly 80% successfully resulting in the receipt of a counterfeit item.<sup>3</sup>*

The scale of counterfeit activity online is evidenced as well by the significant efforts e-commerce platforms themselves have had to undertake. A major e-commerce platform reports that its proactive efforts prevented over 1 million suspected bad actors from publishing a single product for sale through its platform and blocked over 3 billion suspected counterfeit listings from being published to their marketplace. Despite efforts such as these, private sector actions have not been sufficient to prevent the importation and sale of a wide variety and large volume of counterfeit and pirated goods to the American public.

The projected growth of e-commerce fuels mounting fears that the scale of the problem will only increase, especially under a business-as-usual scenario. Consequently, an effective and meaningful response to the President's memorandum is a matter of national import.

#### Actions to be Taken by DHS and the U.S. Government

Despite public and private efforts to-date, the online availability of counterfeit and pirated goods continues to increase. Strong government action is necessary to fundamentally realign incentive structures and thereby encourage the private sector to increase self-policing efforts and focus more innovation and expertise on this vital problem. Therefore, DHS will immediately undertake the following actions and make recommendations for other departments and agencies to combat the trafficking of counterfeit and pirated goods.

<b><i>Immediate Actions by DHS and Recommendations for the U.S. Government</i></b>
<b>1. Ensure Entities with Financial Interests in Imports Bear Responsibility</b>
<b>2. Increase Scrutiny of Section 321 Environment</b>
<b>3. Suspend and Debar Repeat Offenders; Act Against Non-Compliant International Posts</b>
<b>4. Apply Civil Fines, Penalties and Injunctive Actions for Violative Imported Products</b>
<b>5. Leverage Advance Electronic Data for Mail Mode</b>
<b>6. Anti-Counterfeiting Consortium to Identify Online Nefarious Actors (ACTION) Plan</b>
<b>7. Analyze Enforcement Resources</b>
<b>8. Create Modernized E-Commerce Enforcement Framework</b>
<b>9. Assess Contributory Trademark Infringement Liability for Platforms</b>
<b>10. Re-Examine the Legal Framework Surrounding Non-Resident Importers</b>
<b>11. Establish a National Consumer Awareness Campaign</b>

---

<sup>3</sup> International Anti-Counterfeiting Coalition's comments made on the Department of Commerce, International Trade Administration, Office of Intellectual Property Rights', Report on the State of Counterfeit and Pirated Goods Trafficking Recommendations, 29 July 2019. Posted on 6 August 2019. <https://www.regulations.gov/document?D=DOC-2019-0003-0072>

## Best Practices for E-Commerce Platforms and Third-Party Marketplaces

Government action alone is not enough to bring about the needed paradigm shift and ultimately stem the tide of counterfeit and pirated goods. All relevant private-sector stakeholders have critical roles to play and must adopt identified best practices, while redoubling efforts to police their own businesses and supply chains.

While the U.S. brick-and-mortar retail store economy has a well-developed regime for licensing, monitoring, and otherwise ensuring the protections of intellectual property rights (IPR), a comparable regime is largely non-existent for international e-commerce sellers. The following table catalogs a set of high priority “best practices” that shall be communicated to all relevant private sector stakeholders by the National Intellectual Property Rights Coordination Center. It shall be the Center’s duty to monitor and report on the adoption of these best practices within the scope of the legal authority of DHS and the Federal government.

<b><i>Best Practices for E-Commerce Platforms and Third-Party Marketplaces</i></b>
<b>1. Comprehensive "Terms of Service" Agreements</b>
<b>2. Significantly Enhanced Vetting of Third-Party Sellers</b>
<b>3. Limitations on High Risk Products</b>
<b>4. Rapid Notice and Takedown Procedures</b>
<b>5. Enhanced Post-Discovery Actions</b>
<b>6. Indemnity Requirements for Foreign Sellers</b>
<b>7. Clear Transactions Through Banks that Comply with U.S. Enforcement Requests for Information (RFI)</b>
<b>8. Pre-Sale Identification of Third-Party Sellers</b>
<b>9. Establish Marketplace Seller ID</b>
<b>10. Clearly Identifiable Country of Origin Disclosures</b>

Foremost among these best practices is the idea that e-commerce platforms, online third-party marketplaces, and other third-party intermediaries such as customs brokers and express consignment carriers must take a more active role in monitoring, detecting, and preventing trafficking in counterfeit and pirated goods.

## 2. Introduction

*E-commerce platforms represent ideal storefronts for counterfeits...and provide powerful platform[s] for counterfeiters and pirates to engage large numbers of potential consumers.*

- Organisation for Economic Cooperation and Development<sup>4</sup>

The rapid growth of e-commerce platforms, further catalyzed by third-party online marketplaces connected to the platforms, has revolutionized the way products are bought and sold. “Online third-party marketplace” means any web-based platform that includes features primarily designed for arranging the sale, purchase, payment, or shipping of goods, or that enables sellers not directly affiliated with an operator of such platforms to sell physical goods to consumers located in the United States.

In the United States, e-commerce year-over-year retail sales grew by 13.3 percent in the second quarter of 2019 while total retail sales increased by only 3.2 percent as brick-and-mortar retail continued its relative decline.<sup>5</sup> For example, Amazon reports third-party sales on its marketplace grew from \$100 million in 1999 to \$160 billion in 2018.<sup>6</sup> In 2018 alone, Walmart experienced an e-commerce sales increase of 40 percent.<sup>7</sup>

Counterfeits threaten national security and public safety directly when introduced into government and critical infrastructure supply chains, and indirectly if used to generate revenue for transnational criminal organizations. Counterfeits also pose risks to human health and safety, erode U.S. economic competitiveness and diminish the reputations and trustworthiness of U.S. products and producers. Across all sectors of the economy, counterfeit goods unfairly compete with legitimate products and reduce the incentives to innovate, both in the United States and abroad.

While the expansion of e-commerce has led to greater trade facilitation, its overall growth—especially the growth of certain related business models—has facilitated online trafficking in counterfeit and pirated goods. American consumers shopping on e-commerce platforms and online third-party marketplaces now face a significant risk of purchasing counterfeit or pirated goods. This risk continues to rise despite current efforts across e-commerce supply chains to reduce such trafficking.

---

<sup>4</sup> OECD (2018), *Governance Frameworks to Counter Illicit Trade*, Illicit Trade, OECD Publishing, Paris, <https://doi.org/10.1787/9789264291652-en>.

<sup>5</sup> Department of Commerce, U.S. Census Bureau, Economic Indicators Division, “Quarterly Retail E-Commerce Sales 2<sup>nd</sup> Quarter 2019,” 19 August 2019. <https://www2.census.gov/retail/releases/historical/ecomm/19q2.pdf>

<sup>6</sup> Jeff Bezos, “2018 Letter to Shareholders,” *The Amazon Blog*. 11 April 2019. <https://blog.aboutamazon.com/company-news/2018-letter-to-shareholders>

<sup>7</sup> Note: Walmart does not separate out the percentage of third-party vendor sales. More information can be found, *here*, Jaiswal, Abhishek, “Getting Started Selling on Walmart in 2019: An Insider’s Guide to Success,” *BigCommerce*.

<https://www.bigcommerce.com/blog/selling-on-walmart-marketplace/#millennials-are-the-drivers-of-legacy-brand-change-including-walmart>. See also, “Walmart Marketplace: Frequently Asked Questions,” *Walmart*. <https://marketplace.walmart.com/resources/#1525808821038-8edf332b-5ba2>.

The OECD reports international trade in counterfeit and pirated goods amounted to as much as \$509 billion in 2016. This represents a 3.3 percent increase from 2013 as a proportion of world trade. From 2003<sup>8</sup> through 2018, seizures of infringing goods by the U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE) increased from 6,500 to 33,810 while the domestic value of seized merchandise — as measured by manufacturer's suggested retail price of the legitimate good (MSRP) — increased from \$94 million in 2003 to \$1.4 billion in 2018.<sup>9</sup>

The rise in consumer use of third-party marketplaces significantly increases the risks and uncertainty for U.S. producers when creating new products. It is no longer enough for a small business to develop a product with significant local consumer demand and then use that revenue to grow the business regionally, nationally, and internationally with the brand protection efforts expanding in step. Instead, with the international scope of e-commerce platforms, once a small business exposes itself to the benefits of placing products online — which creates a geographic scope far greater than its more limited brand protection efforts can handle — it begins to face increased foreign infringement threat.

Moreover, as costs to enter the online market have come down, such market entry is happening earlier and earlier in the product cycle, further enhancing risk. If a new product is a success, counterfeiters will attempt, often immediately, to outcompete the original seller with lower-cost counterfeit and pirated versions while avoiding the initial investment into research and design.

In other words, on these platforms, the counterfeit and pirated goods compete unfairly and fraudulently against the genuine items. While counterfeit and pirated goods have been sold for years on street corners, alleys, and from the trunks of cars, these illicit goods are now marketed to consumers in their homes through increasingly mainstream e-commerce platforms and third party online marketplaces that convey an air of legitimacy.

With the rise of e-commerce, the problem of counterfeit trafficking has intensified. The OECD documents a 154 percent increase in counterfeits traded internationally, from \$200 billion in 2005 to \$509 billion in 2016.<sup>10</sup> Data collected by CBP between 2000 and 2018 shows that seizures of infringing goods at U.S. borders, much of it trafficked through e-commerce, has increased ten-fold. Over 85 percent of the contraband seized by CBP arrived from China and Hong Kong. These high rates of seizures are consistent with a key OECD finding.

*Counterfeit and pirated products come from many economies, with China appearing as the single largest producing market. These illegal products are frequently found in a range of industries, from luxury items (e.g. fashion apparel or deluxe watches), via intermediary products (such as machines, spare parts or*

---

<sup>8</sup> [https://www.cbp.gov/sites/default/files/documents/FY2003%20IPR%20Seizure%20Statistics\\_0.pdf](https://www.cbp.gov/sites/default/files/documents/FY2003%20IPR%20Seizure%20Statistics_0.pdf).

<sup>9</sup> [https://www.cbp.gov/sites/default/files/assets/documents/2019-Aug/IPR\\_Annual-Report-FY-2018.pdf](https://www.cbp.gov/sites/default/files/assets/documents/2019-Aug/IPR_Annual-Report-FY-2018.pdf)

<sup>10</sup> OECD/EUIPO (2016), Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact, OECD Publishing, Paris.

<https://www.oecd-ilibrary.org/docserver/9789264252653-en.pdf?Expires=1576509401&id=id&accname=id5723&checksum=576BF246D4E50234EAF5E8EDF7F08147>

*chemicals) to consumer goods that have an impact on personal health and safety (such as pharmaceuticals, food and drink, medical equipment, or toys).<sup>11</sup>*

### Operation Mega Flex

In 2019, in response to the alarmingly high rates of contraband uncovered by DHS and a request from the White House Office of Trade and Manufacturing Policy (OTMP), CBP initiated Operation Mega Flex. This operation uses enhanced inspection and monitoring efforts to identify high-risk violators that are shipping and receiving illicit contraband through international mail facilities and express consignment hubs.

The periodic “blitz operations” conducted under the auspices of Operation Mega Flex examine thousands of parcels from China and Hong Kong and carefully catalog the range of contraband seized. To date, such operations have included visits to seven of CBP’s international mail facilities and four express consignment hubs and the completion of over 20,000 additional inspections. The following table summarizes the findings of three Mega Flex blitzes conducted between July and September of 2019.

<b><i>Results of Operation Mega Flex (2019)</i></b>				
	<b>Blitz I July 16 &amp; 17</b>	<b>Blitz II August 21</b>	<b>Blitz III September 18</b>	<b>Total</b>
<b>Inspections</b>	<b>9,705</b>	<b>5,757</b>	<b>5,399</b>	<b>20,861</b>
<b>Discrepancies</b>	<b>1,145</b>	<b>1,010</b>	<b>735</b>	<b>2,890</b>
<b>Discrepancy Rate</b>	<b>11.8%</b>	<b>17.5%</b>	<b>13.6%</b>	<b>13.9%</b>
<b>Counterfeits</b>	<b>212</b>	<b>467</b>	<b>382</b>	<b>1,061</b>
<b>Counterfeit Rate</b>	<b>2.2%</b>	<b>8.1%</b>	<b>7.1%</b>	<b>5.1%</b>

**Source: U.S. Customs and Border Protection**

Among the discrepancies uncovered by Operation Mega Flex were 1,061 shipments of counterfeit products. These counterfeits range from fake name brand items, like Louis Vuitton bags to sports equipment made with faulty parts. Other contraband included drug paraphernalia, deadly opioids, and counterfeit drivers’ licenses.<sup>12</sup> In all, counterfeits constituted more than one of every three discrepancies uncovered by inspectors.<sup>13</sup>

---

<sup>11</sup> OECD/EUIPO (2016), Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact, OECD Publishing, Paris. <https://www.oecd-ilibrary.org/docserver/9789264252653-en.pdf?expires=1576509401&id=id&accname=id5723&checksum=576BF246D4E50234EAF5E8EDF7F08147>

<sup>12</sup> Oren Fliegelman, “Made in China: Fake IDs,” *The New York Times*. 6 February 2015.

<https://www.nytimes.com/2015/02/08/education/edlife/fake-ids-or-why-would-a-student-order-a-tea-set.html>

<sup>13</sup> Among the near 3,000 discrepancies, 20% of them were agricultural violations, such as bad meat, fruit, or produce, unsafe for the American consumer. These agricultural discrepancies are dangerous to the United States because they may contain diseases or pests that can greatly impact agriculture. For example, on October 16, 2018, CBP seized nearly 900 pounds of mitten crabs from an incoming Chinese freight. In Asia, mitten crabs are considered a seasonal delicacy; however, they have a disastrous impact on other global habitats and are labeled as an invasive species. See, Department of Homeland Security, U.S. Customs and Border Protection, “CBP Prevents Smuggling of Nearly 900 Pounds of Invasive Mitten Crabs,” 31 October 2018. <https://www.cbp.gov/newsroom/national-media-release/cbp-prevents-smuggling-nearly-900-pounds-invasive-mitten-crabs>.

Authorities also seized 174 controlled or prohibited substances, including: recreational drugs like LSD, cocaine, DMT, ecstasy, marijuana, mushrooms, and poppy pods as well as steroids and highly addictive painkillers like Tramadol.

It is not just a rise in the volume of counterfeits we are witnessing. GAO notes that counterfeiters are increasingly producing a “wider variety of goods that may be sold on websites alongside authentic products.”<sup>14</sup>

DHS finds the current state of e-commerce to be an intolerable and dangerous situation that must be addressed firmly and swiftly by strong actions within the Department and across other relevant agencies of the U.S. Government (USG). These include: The Federal Bureau of Investigation and the Department of Justice, the Department of Commerce, and the Department of the Treasury. This report provides a blueprint for swift and constructive changes and sets forth several actions for immediate implementation.

### 3. Overview of Counterfeit and Pirated Goods Trafficking

While most e-commerce transactions involve legitimate sellers and products, far too many involve the trafficking of counterfeit and pirated goods and expose legitimate businesses and consumers to substantial risks. This is a global phenomenon; the OECD reports international trade in counterfeit and pirated goods amounted to as much as half a trillion dollars in 2016.<sup>15</sup>

#### Key Drivers of Counterfeiting and Piracy in E-Commerce

Historically, many counterfeits were distributed through swap meets and individual sellers located on street corners. Today, counterfeits are being trafficked through vast e-commerce supply chains in concert with marketing, sales, and distribution networks. The ability of e-commerce platforms to aggregate information and reduce transportation and search costs for consumers provides a big advantage over brick-and-mortar retailers. Because of this, sellers on digital platforms have consumer visibility well beyond the seller’s natural geographical sales area.

Selling counterfeit and pirated goods through e-commerce is a highly profitable activity: production costs are low, millions of potential customers are available online, transactions are convenient, and listing on well-branded e-commerce platforms provides an air of legitimacy.

---

Other discrepancies found by CBP in the blitz operations included 13 weapon modifications and gun parts, 3 occurrences of drug paraphernalia, and 3 pill presses. For full summary of findings, see, Department of Homeland Security, U.S. Customs and Border Protection, Operation Mega Flex I, II and III Summaries, 2019.

<sup>14</sup>U.S. Government Accountability Office Report to the Chairman, Committee on Finance, U.S. Senate: *Intellectual Property: Agencies Can Improve Efforts to Address Risks Posed by Changing Counterfeits Market*, GAO-18-216, Washington, DC: Government Accountability Office, January 2018. <https://www.gao.gov/assets/690/689713.pdf>

<sup>15</sup>See OECD, Trends in Trade in Counterfeit and Pirated Goods (March 2019), available at <https://www.oecd.org/governance/risk/trends-in-trade-in-counterfeit-and-pirated-goods-g2g9f533-en.htm>

<sup>15</sup>See Parker et al. 2016

When sellers of illicit goods are in another country, they are largely outside the jurisdiction for criminal prosecution or civil liability from U.S. law enforcement and private parties.

#### *The Role of Online Third-Party Marketplaces*

Third-party online marketplaces can quickly and easily establish attractive “store-fronts” to compete with legitimate businesses. On some platforms, little identifying information is necessary to begin selling.

A counterfeiter seeking to distribute fake products will typically set up one or more accounts on online third-party marketplaces. The ability to rapidly proliferate third-party online marketplaces greatly complicates enforcement efforts, especially for intellectual property rights holders. Rapid proliferation also allows counterfeiters to hop from one profile to the next even if the original site is taken down or blocked. On these sites, online counterfeiters can misrepresent products by posting pictures of authentic goods while simultaneously selling and shipping counterfeit versions.

Counterfeiters have taken full advantage of the aura of authenticity and trust that online platforms provide. While e-commerce has supported the launch of thousands of legitimate businesses, their models have also enabled counterfeiters to easily establish attractive “store-fronts” to compete with legitimate businesses.

Platforms use their third-party marketplace functions to leverage “two-sided” network effects to increase profitability for the platform by adding both more sellers and more buyers. Because sellers benefit with each additional buyer using the platform (more consumers to sell to), and buyers are more likely to join/use the platform with each additional seller (more sellers to buy from), there can be diminished internal resistance to adding lower quality sellers.

Platforms that recognize this strategy may incentivize seller listings to stimulate further growth and increase profits but do so without adequate scrutiny. As just one incentive, many platforms create “frictionless entry” by reducing the costs for sellers and buyers to join, thereby increasing the likelihood that the platform will reach an efficient and highly profitable scale.

Platforms also generate value by opening previously unused (or less frequently used) markets. In addition, online platforms reduce transaction costs by streamlining the actual transaction; for example, buyers and sellers use a standardized transaction method that simplifies interactions with buyers and reduces the risk that the buyer will not pay.

For example, before the rise of e-commerce, secondhand products could be sold at garage sales or in classified newspaper advertisements. E-commerce created a process for allowing buyers and sellers to trade goods digitally, reducing transaction costs and creating a global marketplace for used, but too often counterfeit, products.

Another way platforms generate value is by aggregating information and reducing search costs. A buyer may search for a product, either by keyword or product category, at lower search cost than visiting brick-and-mortar stores. Because of this, sellers on digital platforms have consumer visibility well beyond the seller’s natural geographical sales area.

In addition, consumers who have made a purchase may use tools provided by the marketplace to rate the product and the seller involved. These ratings create an important mechanism to facilitate future consumer trust in an otherwise unknown seller.

In principle, such a rating system provides a key to overcoming a common economic problem that might otherwise preclude sales: without a low-cost trust building feature that also communicates quality, and in a market with significant numbers of low-quality products, buyers may refuse to purchase any product at all, or would demand a lower price to reflect the uncertainty. One frequent result is that low cost counterfeits drive out high quality, trusted brands from the online marketplace. In practice, even the ratings systems across platforms have been gamed, and the proliferation of fake reviews and counterfeit goods on third-party marketplaces now threatens the trust mechanism itself.

#### *Lower Startup and Production Costs*

The relative ease of setting up and maintaining e-commerce websites makes online marketplaces a prime locale for the retailing of counterfeit and pirated goods. E-commerce retailers enjoy low fixed costs of setting up and maintaining web businesses and lower costs for carrying out normal business operations such as managing merchant accounts. These ventures can be set up quickly without much sophistication or specialized skills.

Some online platforms allow retailers to use pre-made templates to create their stores while other platforms only require that a seller create an account. These businesses face much lower overhead costs than traditional brick-and-mortar sellers because there is no need to rent retail space or to hire in-person customer-facing staff. Not only can counterfeiters set up their virtual storefronts quickly and easily, but they can also set up new virtual storefronts when their existing storefronts are shut down by either law enforcement or through voluntary initiatives set up by other stakeholders such as market platforms, advertisers, or payment processors.

In the production stage, counterfeiters keep costs low by stealing product secrets or technological knowledge, exploiting new production technologies, and distributing operations across jurisdictions. One method involves employees who sell trade secrets to a third party who, in turn, develops and sells counterfeit products based on the stolen secrets. Another method relies on an intermediary to steal a firm's product or technology. The use of intermediaries reduces the traceability to the counterfeiter.

Counterfeiting and piracy operations also take advantage of new low-cost production technologies. For example, the technological advances in modeling, printing and scanning technologies such as 3D printing reduce the barriers for reverse engineering and the costs of manufacturing counterfeit products.

Lower production costs can also be achieved through distributed production operations. One method involves manufacturing the counterfeit good in a foreign market to lower the chances of detection and to minimize legal liability if prosecuted. This can be combined with importation of

the counterfeit labels separately from the items, with the labels being applied to the products after both items arrive in the U.S.

In addition, it is much cheaper to manufacture illicit goods because counterfeit and pirated goods are often produced in unsafe workplaces with substandard and unsafe materials by workers who are often paid little—and sometimes nothing in the case of forced labor. Moreover, in the case of goods governed by Federal health and safety regulations, it often costs much less to produce counterfeit versions that do not meet these health and safety standards.

#### *Lower Marketing Costs*

Businesses that use only an internet presence as their consumer-facing aspect typically enjoy lower costs of designing, editing, and distributing marketing materials. Counterfeitors also benefit from greater anonymity on digital platforms and web sites and greater ease to retarget or remarket to customers. For example, counterfeiters use legitimate images and descriptions on online platforms to confuse customers, and they open multiple seller accounts on the platform so that if one account is identified and removed, the counterfeiter can simply use another.

The popularity of social media also helps reduce the costs of advertising counterfeit products. The nature of social media platforms has aided in the proliferation of counterfeits across all e-commerce sites. Instagram users, for example, can take advantage of connectivity algorithms by using the names of luxury brands in hashtags. Followers can search by hashtag and unwittingly find counterfeit products, which are comingled and difficult to differentiate from legitimate products and sellers.

#### *Lower Distribution Costs*

Traditionally, many counterfeit goods were distributed through swap meets and individual sellers located on street corners. With the rise of online platforms for shopping, customers can have products delivered to them directly.

Foreign entities that traffic in counterfeits understand how to leverage newer distribution methods better suited to e-commerce than the traditional trade paradigm (i.e., imports arriving via large cargo containers with domestic distribution networks). Today, mail parcel shipments, including through express consignments, account for more than 500 million packages each year.<sup>16</sup> Seizures in the small package environment made up 93 percent of all seizures in 2018, a 6 percent increase over 2017. From 2012 to 2016, the number of seizures from express consignment carriers increased by 105 percent, and the MSRP of those seizures had a 337 percent increase.<sup>17</sup> In contrast, seizures from cargo decreased by 36 percent from FY17 to FY18.

---

<sup>16</sup><https://www.cbp.gov/sites/default/files/assets/documents/2019-Apr/FY%202017%20Seizure%20Stats%20Booklet%20-%20508%20Compliant.pdf> p. 14

<sup>17</sup>[https://www.gao.gov/assets/690/689713.pdf?mod=article\\_inline](https://www.gao.gov/assets/690/689713.pdf?mod=article_inline) p. 14

The International Chamber of Commerce found that counterfeiters use international air packages because the high volume of these packages makes enforcement more difficult.<sup>18</sup> A recent report by the OECD points out that distributing counterfeits across a series of small packages spreads the risk of detection, and lowers the loss from having one or more shipments seized, suggesting that losses to the counterfeiter on an ongoing basis would be within a tolerable range.<sup>19</sup>

The OECD report also notes that it is harder for authorities to detect counterfeits in small parcels than in shipping containers because cargo containers making entry at a maritime port provide customs officials with more information, well in advance of arrival. Moreover, the effort required for CBP to seize a shipment does not vary by size of the shipment, meaning that a package of a few infringing goods requires the same resources to seize as a cargo container with hundreds of infringing goods.

Section 321 of the Tariff Act of 1930 has likewise encouraged counterfeiters to favor smaller parcel delivery. Under Section 321, a foreign good valued at or less than \$800 and imported by one person on one day is not subject to the same formal customs entry procedures and rigorous data requirements as higher-value packages entering the United States. This reduced level of scrutiny is an open invitation to exploit Section 321 rules to transport and distribute counterfeits.

Rules set by the Universal Postal Union (UPU) have historically contributed to the distortion in rates for delivery of international e-commerce purchases to the United States.<sup>20</sup> UPU reimbursement rates have underpriced domestic postage rates for small parcels. This market distortion made it cheaper for small package exports to the United States from certain countries than would otherwise be economically feasible and has encouraged the use of the international postal mode over other shipment channels. The United States recently scored a historic victory when the UPU overhauled its terminal dues system<sup>21</sup>, effectively eliminating this outdated policy.<sup>22</sup>

### *Consumer Attitudes and Perceptions*

The sale of counterfeits away from so-called “underground” or secondary markets (e.g. street corners, flea markets) to e-commerce platforms is reshaping consumer attitudes and perceptions. Where in the past, consumers could identify products by relying on “red flag” indicators—such as a suspicious location of the seller, poor quality packaging, or discount pricing—consumers are now regularly exposed to counterfeit products in settings and under conditions where the articles appear genuine.

While the risks of receiving a counterfeit may have been obvious to a consumer purchasing items on street corners, with the rise of online platforms, it is not so obvious anymore. For example, it is

---

<sup>18</sup><https://cdn.iccwbo.org/content/uploads/sites/3/2015/03/ICC-BASCAP-Roles-and-Responsibilities-of-Intermediaries.pdf> p. 32

<sup>19</sup>OECD/EUIPO (2018), *Misuse of Small Parcels for Trade in Counterfeit Goods: Facts and Trends, Illicit Trade*, OECD Publishing, Paris. <https://doi.org/10.1787/9789264307858-en> p. 77

<sup>20</sup>The UPU is a specialized agency of the United Nations that coordinates postal policies between 190 countries. Importantly, these treaties determine the cost of shipping between the various countries and offers low rates to mail originating from abroad, as compared to domestic postage rates.

<sup>21</sup> Universal Postal Union (2019), *Decisions of the 2019 Geneva Extraordinary Congress*, [http://www.upu.int/uploads/tx\\_sbdownloader/actsActsOfTheExtraordinaryCongressGenevaEn.pdf](http://www.upu.int/uploads/tx_sbdownloader/actsActsOfTheExtraordinaryCongressGenevaEn.pdf)

<sup>22</sup> <https://www.nytimes.com/2019/09/25/business/universal-postal-union-withdraw.html>

unlikely that anyone would set out to purchase a counterfeit bicycle helmet given the potential safety risks; however, such items are readily available to unsuspecting consumers on e-commerce websites.

Reports indicate that some third-party marketplace listings falsely claim to have certifications with health and safety standards or offer items banned by federal regulators or even the platforms themselves. Coupled with the inability of buyers to accurately determine the manufacturer or the origin of the product, it is challenging for buyers to make informed decisions in the e-commerce environment.

In 2017, MarkMonitor found that 39 percent of all unwitting purchases of counterfeit goods were bought through online third-party marketplaces.<sup>23</sup> Sellers on large well-known platforms rely on the trust that those platforms hosting of the marketplace elicits. The results of this survey indicate that bad actors selling counterfeit goods on legitimate online platforms erodes trust in both the brands and the platforms themselves.

In 2018, Incopro conducted a survey focusing on United Kingdom (UK) consumers who had unwittingly purchased counterfeit goods and how their perceptions of online marketplaces were affected as a result.<sup>24</sup> The results of this survey show that 26 percent of respondents reported that they had unwittingly purchased counterfeits. Of these, 41 percent reported that they had never received a refund after reporting a seller to online marketplaces.

In addition, roughly one-third of respondents reported that they would be less likely to buy a widely counterfeited product from an online marketplace while 46 percent reported no longer using a particular online marketplace after receiving counterfeit goods. Respondents also reported that, when trying to differentiate between genuine and counterfeit products, they consider online reviews along with the reputation of online marketplaces.

These recent findings, against the larger backdrop of the e-commerce environment, demonstrate the immediacy of the problem as consumer confidence and brand integrity continue to suffer in the realm of online third-party marketplaces.

### Top Products Prone to Counterfeiting and Piracy

Counterfeitors sell fake goods as authentic goods — for example, a copy of a Louis Vuitton bag or Rolex watch fraudulently sold as the “real thing.” Counterfeitors use identical copies of registered trademarks without the authorization of the rightful owner.

Piracy typically refers to the act of copying a protected work (such as a book, movie, or music) without the consent of the rights holder or person duly authorized by the rights holder.

---

<sup>23</sup>MarkMonitor (2017). *MarkMonitor Online Barometer: Global online shopping survey 2017 – consumer goods*. Downloaded from [https://www.markmonitor.com/download/report/MarkMonitor\\_Online\\_Shopping\\_Report-2017-UK.pdf](https://www.markmonitor.com/download/report/MarkMonitor_Online_Shopping_Report-2017-UK.pdf). p. 6

<sup>24</sup>INCOPRO, 2018. Counterfeit Products are Endemic – and it is damaging brand value: INCOPRO Market Research Report available at [https://www.incoproip.com/cms/wp-content/uploads/2018/11/2018\\_Incopro\\_Market-Research-report.pdf](https://www.incoproip.com/cms/wp-content/uploads/2018/11/2018_Incopro_Market-Research-report.pdf).

were between 2 million and 2.6 million jobs in 2013, with job displacement expected to double by 2022.

Counterfeit goods also damage the value of legitimate brands. When brand owners lose the ability to collect a price premium for branded goods, it leads to diminished innovation as brand owners are less likely to invest in creating innovative products. Legitimate companies, and particularly small businesses, report devastating impacts due to the abundance of competing online counterfeits and pirated goods. Moreover, while e-commerce platforms can benefit legitimate businesses by helping them to reach customers with a new product, the same process and technology also makes it easier for unscrupulous firms to identify popular new products, produce infringing versions of them, and sell these illicit goods to the business's potential customers.

As previously noted, the speed at which counterfeiters can steal intellectual property through e-commerce can be very rapid. If a new product is a success, counterfeiters may attempt to immediately outcompete the original seller with lower-cost counterfeit versions — while avoiding research and development costs. The result: counterfeiters may have a significant competitive advantage in a very short period of time over those who sell trusted brands.

Such fast-track counterfeiting poses unique and serious problems for small businesses, which do not have the same financial resources as major brands to protect their intellectual property. Lacking the ability to invest in brand-protection activities, such as continually monitoring e-commerce platforms to identify illicit goods, perform test buys, and send takedown notices to the platforms, smaller businesses are more likely to experience revenue losses as customers purchase counterfeit versions of the branded products.

In many cases, American enterprises have little recourse aside from initiating legal action against a particular vendor. Such legal action can be extremely difficult. Many e-commerce sellers of infringing products are located outside the jurisdiction of the United States, often in China; existing laws and regulations largely shield foreign counterfeiters from any accountability.

## **Organized Crime and Terrorism**

The impact of counterfeit and pirated goods is broader than just unfair competition. Law enforcement officials have uncovered intricate links between the sale of counterfeit goods and transnational organized crime. A study by the Better Business Bureau notes that the financial operations supporting counterfeit goods typically require central coordination, making these activities attractive for organized crime, with groups such as the Mafia and the Japanese Yakuza heavily involved.<sup>33</sup> Criminal organizations use coerced and child labor to manufacture and sell counterfeit goods. In some cases, the proceeds from counterfeit sales may be supporting terrorism and dictatorships throughout the world.<sup>34</sup>

---

<sup>33</sup>[https://www.bbb.org/globalassets/local-bbbs/st-louis-mo-142/st\\_louis\\_mo\\_142/studies/counterfeit-goods/BBB-Study-of-Counterfeit-Goods-Sold-Online.pdf](https://www.bbb.org/globalassets/local-bbbs/st-louis-mo-142/st_louis_mo_142/studies/counterfeit-goods/BBB-Study-of-Counterfeit-Goods-Sold-Online.pdf)

<sup>34</sup>United Nations Office of Drugs and Crime (UNODC), *Focus On: The Illicit Trafficking of Counterfeit Goods and Transnational Organized Crime*, available at: [https://www.unodc.org/documents/counterfeit/FocusSheet/Counterfeit\\_focussheet\\_EN\\_HIRES.pdf](https://www.unodc.org/documents/counterfeit/FocusSheet/Counterfeit_focussheet_EN_HIRES.pdf)

## National Security

One of the greatest threats counterfeits pose to national security is their entry into the supply chain of America's defense industrial base. This defense industrial base includes both private sector contractors and government agencies, particularly the Department of Defense.

In FY 2018, 12 percent of DHS seizures included counterfeit versions of critical technological components, automotive and aerospace parts, batteries, and machinery. Each of these industrial sectors have been identified as critical to the defense industrial base, and thus critical to national security. One example drawn from a 2018 study by the Bureau of Industry and Security within the Department of Commerce featured the import of counterfeit semiconductors or "Trojan chips" for use in defense manufacturing and operations<sup>35</sup>. Such Trojan chips can carry viruses or malware that infiltrate and weaken American national security. The problem of counterfeit chips has become so pervasive that the Department of Defense has referred to it as an "invasion." Companies from China are the primary producers of counterfeit electronics.<sup>36</sup>

## 5. How E-Commerce Facilitates Counterfeit Trafficking

While e-commerce has supported the launch of thousands of legitimate businesses, e-commerce platforms, third-party marketplaces, and their supporting intermediaries have also served as powerful stimulants for the trafficking of counterfeit and pirated goods. The central economic driver of such trafficking is this basic reality: Selling counterfeit and pirated goods through e-commerce platforms and related online third-party marketplaces is a highly profitable venture.

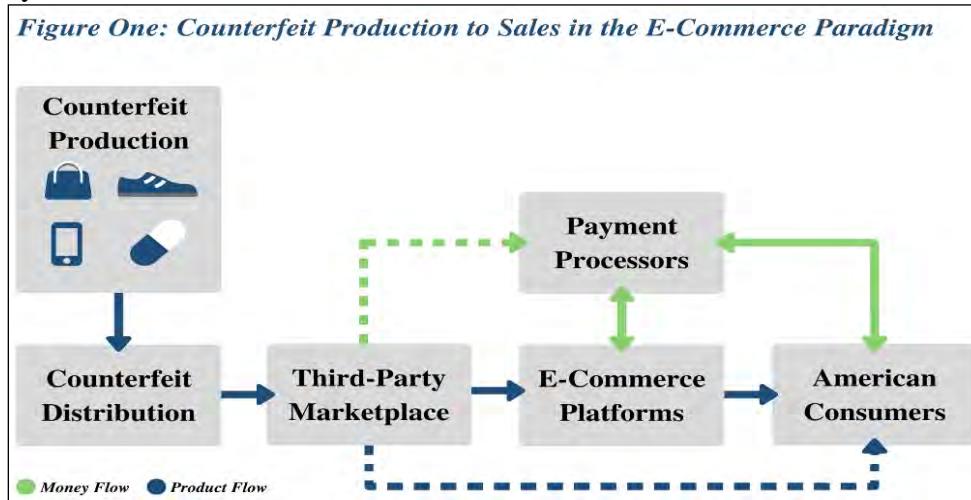
For counterfeiters, production costs are low, millions of potential customers are available online, transactions are convenient, and listing goods on well-known platforms provides an air of legitimacy. When sellers of illicit goods are in another country, they are also exposed to relatively little risk of criminal prosecution or civil liability under current law enforcement and regulatory practices. It is critical that immediate action be taken to protect American consumers and other stakeholders against the harm and losses inflicted by counterfeiters.

---

<sup>35</sup><https://www.bis.doc.gov/index.php/documents/technology-evaluation/37-defense-industrial-base-assessment-of-counterfeit-electronics-2010/file>

<sup>36</sup>Saunders, Gregory and Tim Koczanski, "Counterfeits," *Defense Standardization Program Journal*, October/December 2013. <https://www.dsp.dla.mil/Portals/26/Documents/Publications/Journal/131001-DSPJ.pdf>

Figure One provides a simplified overview of how counterfeit products move from production by counterfeiters to sales to American consumers:



### Counterfeit Production and Distribution

The counterfeit sales process begins with some type of production capability for the counterfeit good. In this stage, counterfeiters enjoy enormous production cost advantages relative to legitimate businesses. Counterfeits are often produced in unsafe workplaces, with substandard and unsafe materials, by workers who are often paid little or sometimes nothing in the case of forced labor.

In the case of goods subject to federal health and safety regulations, it costs much less to produce counterfeit versions that do not meet these health and safety requirements that make the legitimate products so safe.

Counterfeitors likewise minimize the need for incurring significant research and development expenditures by stealing intellectual property, technologies, and trade secrets. They also shave production costs using inferior ingredients or components.

For example, a common way for counterfeiters to produce *fake* prescription opioids like Oxycontin, or a prescription drug like Viagra, is to start with the *real* pills as a basic ingredient. These real pills are then ground up into a powder, diluted with some type of (sometimes toxic) powder filler, and then “spiked” with an illegal and deadly narcotic like fentanyl, in the case of fake opioids, or illegal and deadly amphetamines or strychnine, in the case of Viagra.

In the case of apparel, such as running shoes, employees from a legitimate branded company may leave the company and set up their own facility. These employees have the expertise to manufacture identical-looking shoes; but they will typically do so with cheaper, inferior components. The result: the shoes may fail during activity, injure the user with an inferior insole, or, at a minimum, wear out faster than the real product.<sup>37</sup>

<sup>37</sup>Department of Homeland Security, U.S. Customs and Border Protection, “CBP Seizes Over \$2.2 Million worth of Fake Nike Shoes at LA/Long Beach Seaport,” 9 October 2019. <https://www.cbp.gov/newsroom/local-media-release/cbp-seizes-over-22-million-worth-fake-nike-shoes-lalong-beach-seaport>

The technological advances in modeling, printing, and scanning technologies such as 3D printing, have also significantly reduced the barriers for reverse engineering and the costs of manufacturing counterfeit products. Again, one problem that may arise may be the use of inferior production inputs that lead to product failure.

These are just a few of the many ways counterfeits begin their long journey into American households. There is often no way for legitimate businesses to compete, on a production cost basis, with counterfeiters. There is also often no way for a consumer to tell the difference between a counterfeit and legitimate good.

### Third-Party Marketplaces and Counterfeiter Websites

A counterfeiter seeking to distribute fake products will typically set up one or more accounts on third-party marketplaces, and these accounts can often be set up quickly and without much sophistication or many specialized skills. Under such circumstances, it is axiomatic that online retailers face much lower overhead costs than traditional brick-and-mortar sellers. There is no need to rent retail space or to hire in-person, customer-facing staff.

In a common scenario, third-party marketplace websites contain photos of the real product, fake reviews of the counterfeit product, and other such disinformation designed to mislead or fool the consumer into believing the legitimacy of the product. The proliferation of such disinformation is the hallmark of the successful online counterfeiter. Such deception not only provides counterfeiters with an enormous competitive advantage over their brick-and-mortar counterparts; legitimate sellers on the internet are harmed as well.

In some cases, counterfeiters hedge against the risk of being caught and their websites taken down from an e-commerce platform by preemptively establishing multiple virtual store-fronts. A key underlying problem here is that on at least some e-commerce platforms, little identifying information is necessary for a counterfeiter to begin selling. In the absence of full transparency, counterfeiters can quickly and easily move to a new virtual store if their original third-party marketplace is taken down.

The popularity of social media also helps proliferate counterfeits across various e-commerce platforms. Instagram users, for example, can take advantage of connectivity algorithms by using the names of luxury brands in hashtags. Followers can search by hashtag and unwittingly find counterfeit products, which are comingled and difficult to differentiate from legitimate products and sellers.

According to a 2019 report, *Instagram and Counterfeiting*, nearly 20 percent of the posts analyzed about fashion products on Instagram featured counterfeit or illicit products.<sup>38</sup> More than 50,000 Instagram accounts were identified as promoting and selling counterfeits, a 171 percent increase from a prior 2016 analysis. Instagram's Story feature, where content disappears in twenty-four hours, was singled out as particularly effective for counterfeit sellers.

---

<sup>38</sup>Stroppa, Andrea, *et al.*, "Instagram and counterfeiting in 2019: new features, old problems," *Ghost Data*, 9 April 2019. Rome, New York. [https://ghostdata.io/report/Instagram\\_Counterfeiting\\_GD.pdf](https://ghostdata.io/report/Instagram_Counterfeiting_GD.pdf)

A more recent development on social media is the proliferation of “hidden listings” for the sale of counterfeits. Social media is used to provide direct hyperlinks in private groups or chats to listings for counterfeit goods that purport to be selling unrelated legitimate items. By accessing the link, buyers are brought to an e-commerce platform which advertises an unrelated legitimate item for the same price as the counterfeit item identified in the private group or chat. The buyer is directed to purchase the unrelated item in the listing but will receive the sought-after counterfeit item instead.

#### Order Fulfillment in E-Commerce

The foreign counterfeiter must first choose between sending a package either by express consignment carrier or through the international post. As a general proposition, express consignment shippers — such as DHL Express, Federal Express, and the United Parcel Service — were subject to data requirements before they were extended to the international posts.

In the next step along the delivery chain, a parcel will arrive at a port of entry under the authority of CBP. Millions of parcels arrive daily, and it is impossible to inspect more than a very small fraction.

Although ocean shipping is still a major mode of transport for counterfeits, the rapid growth of other modes, such as truck and air parcel delivery, threaten to upend established enforcement efforts, and as such, is increasingly used by international counterfeiters. This continued shift from bulk cargo delivery to other modes by counterfeiters is illustrated in the trends in seizure statistics.

It is clear from these observations that counterfeit traffickers have learned how to leverage newer air parcel distribution methods that vary from the traditional brick-and-mortar retail model (for example, imports arriving via large cargo containers with domestic distribution networks). This is an issue that must be directly addressed by firm actions from CBP.

#### Section 321 De Minimis Exemption and Counterfeit Trafficking

Under Section 321 of the Tariff Act of 1930, as amended by the Trade Facilitation and Trade Enforcement Act of 2015 (TFTEA), articles with a value of \$800 or less, imported by one person on one day, can be admitted free of duty and taxes. Under 19 CFR § 10.151 and 19 CFR part 143, Subpart C, those importations are often not subject to the same formal customs procedures and rigorous data requirements as higher-value packages entering the United States. Instead, the low-value shipments can be admitted into U.S. commerce with the presentation of a bill of lading or a manifest listing each bill of lading and a limited data set. The relatively limited nature of the data requirements complicates the identification of high-risk goods by CBP and other enforcement agencies. Under 19 CFR § 143.22, CBP has existing authority to require formal entry (and the complete data set for any shipment) for any merchandise, if deemed necessary for import admissibility enforcement purposes; revenue protection; or the efficient conduct of customs business.

## 9. Assess Contributory Trademark Infringement Liability for E-Commerce

Online platforms have avoided civil liability for contributory trademark infringement in several cases. Given the advance and expansion of e-commerce, DHS recommends that the Department of Commerce consider the following measures:

- Assess the state of liability for trademark infringement considering recent judicial opinions, and the impact of this report—including platforms’ implementation of the best practices directed herein.
- Seek input from the private sector and other stakeholders as to the application of the traditional doctrines of trademark infringement to the e-commerce setting, including whether to pursue changes in the application of the contributory and/or vicarious infringement standards to platforms.

## 10. Re-Examine the Legal Framework Surrounding Non-Resident Importers

Currently, non-resident importers can legally enter goods into the United States provided they have a “resident agent” as defined in regulation. In practice, it can be difficult to compel non-resident importers to pay civil penalties and respond to other enforcement actions available to the USG. With this in mind, DHS should reevaluate the legal framework for allowing non-resident importers in the Section 321 *de minimis* low-value shipment environment.

## 11. Establish a National Consumer Awareness Campaign

Given the critical role that consumers can play in the battle against online counterfeiting, DHS recommends the development of a national public-private awareness campaign. The national public awareness campaign recommended by DHS should involve platforms, rights holders, and the applicable government agencies to provide education for consumers regarding the risks of counterfeits as well as the various ways consumers can use to spot counterfeit products. At present, many consumers remain uninformed as to the risks of buying counterfeit and pirated products online. These risks are both direct to them (e.g., tainted baby food), as well as indirect (e.g., sales revenues can fund terrorism).

Many consumers are also unaware of the significant probabilities they face of being defrauded by counterfeiters when they shop on e-commerce platforms. As this report has documented, these probabilities are unacceptably high and appear to be rising. Even those consumers motivated to conduct research and stay informed might lack the specialized knowledge and efficient user tools to make diligent online buying decisions.

A strong and ongoing national campaign to increase public awareness about the risks of counterfeits in an e-commerce world should help alert consumers about the potential dangers of some online purchases. To the extent e-commerce platforms empower their consumers to participate in the monitoring and detection of counterfeits, e.g., by implementing several of the best practices recommended in this report, this will also help in the fight against the trafficking in counterfeit and pirated goods.

This effort could use technology as well as provide online education. For example, online marketplaces could prominently display messages on their home pages, as well as on high-risk item pages, warning customers about the dangers of counterfeits and urging respect for intellectual property rights. Additionally, the campaign could be paired with technologically-enabled assurances of authenticity. Such an approach would provide commercial advantages to the platforms that adopt it while also benefiting consumers and rights holders through reliable methods to identify and certify the authenticity of branded products across online platforms.

## 8. Private Sector Best Practices

The following table catalogs a set of high priority “best practices” that should be swiftly adopted by e-commerce platforms that operate third-party marketplaces, and other third-party intermediaries. Under the authority of the Secretary of the Department of Homeland Security, these best practices shall be recommended and communicated to all relevant private sector stakeholders by the ICE/HSI-led IPR Center.

It shall be a duty of the IPR Center to encourage, monitor, and report on the adoption of, and the progress and effectiveness of, these best practices, through all means necessary within the scope of the legal authority of DHS and the Federal Government.

<b><i>Best Practices for E-Commerce Platforms and Third-Party Marketplaces</i></b>
1. Comprehensive "Terms of Service" Agreements
2. Significantly Enhanced Vetting of Third-Party Sellers
3. Limitations on High Risk Products
4. Efficient Notice and Takedown Procedures
5. Enhanced Post-Discovery Actions
6. Indemnity Requirements for Foreign Sellers
7. Clear Transactions Through Banks that Comply with U.S. Enforcement Requests
8. Pre-Sale Identification of Third-Party Sellers
9. Establish Marketplace Seller IDs
10. Clearly Identifiable Country of Origin Disclosures

### 1. Comprehensive “Terms of Service” Agreements

It is critical that platforms require all third-party sellers to sign comprehensive and stringent terms of service agreements that maximize the authorities of the platforms to combat counterfeit

trafficking. Terms of service agreements will provide platforms with an important legal means to combat counterfeit trafficking

Most obviously, these terms of service should incorporate explicit prohibitions on selling counterfeit and pirated goods. Once the platform has affirmatively detected infringement on a seller profile, the actions listed below under the category of “post-discovery actions” should be allowed under the terms and taken swiftly.

The terms of service should also list the potential repercussions sellers face for violations. Generally, these repercussions should allow platforms to impose sanctions such as suspension, termination, and debarment without waiting for a determination by a court for sellers who violate the terms of the agreement. The terms should include escalating capabilities to suspend, terminate, and debar counterfeit traffickers and their affiliates.

Specifically, they should allow the platform to conduct, at a minimum, the following actions in response to violations or identified risk factors in the seller’s profile and product postings without waiting for a determination by a court:

- (1) terminate or suspend a seller account based on the use or reference to a username that is confusingly similar to a registered trademark;
- (2) take down or suspend and keep down individual product postings based on the misuse of photographs, logos, external links to infringing content, certain coded messages with actual intellectual property references removed, or imbedded offers to manufacture; and
- (3) allow for an escalating enforcement structure that results in (for major infractions and/or repeat minor infractions) permanent removal of the seller, and any known related seller profiles, from the marketplace feature of the platform and further results in forfeiture and destruction of all offending goods in warehouses or fulfillment centers operated by, or under the control of, the platform.

To maximize platform authorities, and as explained further below, such terms of service should also allow platforms to impose appropriate limitations on products listed, require clearly identifiable country of origin disclosures, impose U.S. banking and indemnity requirements, and significantly improve pre-sale identification of third-party sellers.

## 2. Significantly Enhanced Vetting of Third-Party Sellers

Significantly enhanced vetting of third-party sellers is one of the most effective forms of due diligence platforms can engage in to reduce the risk of counterfeits entering the e-commerce stream. Platforms should have a uniform and articulable vetting regime to determine if a seller will be allowed to list products for sale.

To facilitate enhanced vetting, platforms should, at a minimum, require the following:

- (1) sufficient identification of the seller, its accounts and listings, and its business locations prior to allowing the seller to list products on the platform;
- (2) certification from the seller as to whether it, or related persons, have been banned or removed from any major e-commerce platforms, or otherwise implicated in selling counterfeit or pirated products online; and
- (3) acknowledgment, where applicable, that the seller is offering trademarked products for which the seller does not own the rights (either because they are a reseller or seller of used products).

Information provided by potential sellers should also be vetted for accuracy, including through the following efforts:

- (1) use of technological tools, as well as analyses of historical and public data, to assess risk of sellers and products; and
- (2) establishment of an audit program for sellers, concentrating on repeat offenders and those sellers exhibiting higher risk characteristics.

Any failure to provide accurate and responsive information should result in a determination to decline the seller account and/or to hold the seller in violation of the platform's terms of service.

### 3. Limitations on High Risk Products

Platforms should have in place protocols and procedures to place limitations on the sale of products that have a higher risk of being counterfeited or pirated and/or pose a higher risk to the public health and safety. For example, some of the major platforms completely prohibit the sale of prescription medications by third-party sellers in their marketplaces. Many platforms also ban the sale of products that are known to be particularly vulnerable to counterfeiting and that pose a safety risk when sold online. Examples include car airbag components, infant formula, and new batteries for cellular phones.

Platforms can also place other types of restrictions on third-party sellers before certain high-risk categories of goods may be sold. For example, some platforms require prior approval for items such as automotive parts, jewelry, art, food, computers, sports collectibles, DVDs, and watches that are particularly prone to counterfeiting.

Platforms should prominently publish a list of items that may not be sold on third-party marketplaces under any circumstances (prohibited), as well as a list of items that can only be sold when accompanied by independent third-party certification (restricted). In constructing these lists, platforms should consider, among other things, whether a counterfeit version of the underlying product presents increased risks to the health and safety of U.S. residents or the national security of the United States. When a seller claims their merchandise has an independent third-party certification, and this certification is required in order for the product to be legally offered for sale

in the United States, platforms should make good-faith efforts to verify the authenticity of these certifications.

#### 4. Efficient Notice and Takedown Procedures

Notice and takedown is the most common method of removing counterfeit listings from third-party marketplaces and e-commerce platforms. This noticing process can be particularly time-consuming and resource-intensive for rights holders who currently bear a highly disproportionate share of the burden of identifying the counterfeit listings for noticing.

These rights holders must invest significant resources to scour millions of listings across multiple platforms to identify potentially counterfeit listings and notify the third-party marketplace or e-commerce platform. This kind of comprehensive policing of e-commerce often is not possible for smaller enterprises.

As a further burden, some third-party marketplaces require rights holders to buy the suspected products from the sellers to verify that they are in fact counterfeit. There often is a delay of a day or longer between the time that notice is provided, and the time listing is removed. During this period, counterfeiters may continue to defraud American consumers.

To address these abuses — and assume a much greater share of responsibility for the policing of e-commerce — platforms should create and maintain clear, precise, and objective criteria that allow for quick and efficient notice and takedowns of infringing seller profiles and product listings. An effective regime should include, at a minimum, the following: (1) minimal registration requirements for an interested party to participate in the notice and takedown process; (2) reasonable rules that treat profile owners offering large quantities of goods on consumer-to-consumer platforms as businesses; and (3) transparency to the rights holders as to how complaints are resolved along with relevant information on other sales activity by the seller that has been implicated.

#### 5. Enhanced Post-Discovery Actions

Upon discovery that counterfeit or pirated goods have been sold, platforms should conduct a series of “post-discovery” actions to remediate the fraud. These should include:

- (1) notification to any buyer(s) likely to have purchased the goods in question with the offer of a full refund;
- (2) notification to implicated rights holders, with details of the infringing goods, and information as to any remaining stock of the counterfeit and pirated goods held in warehouses;
- (3) implementation of practices that result in the removal of counterfeit and pirated goods within the platform’s effective control and in a manner that prevents such goods from re-entering the U.S. or being diverted to other markets; and

(4) immediate engagement with law enforcement to provide intelligence and to determine further courses of action.

## 6. Indemnification Requirements for Foreign Sellers

For a large portion of e-commerce, foreign sellers do not provide security or protection against a loss or other financial burden associated with the products they sell in the United States. Because these sellers are located outside the United States, they also may not be subject to the jurisdiction of U.S. courts in civil litigation or government enforcement actions. Further adding to this liability gap, there is this: while e-commerce platforms generally have a U.S. presence and are under U.S. jurisdiction, under the current interpretations of American laws and regulations, they are often found not to be liable for harm caused by the products they sell or distribute.

The result of this jurisdictional and liability gap is that consumers and rights holders do not have an efficient or predictable form of legal recourse when they are harmed by foreign products sold on third-party marketplaces. Accordingly, e-commerce platforms should require foreign sellers to provide some form of security in cases where a foreign product is sold to a U.S. consumer. Such form of security should be specifically designed to cover the potential types and scope of harm to consumers and rights holders from counterfeit or pirated products.

Note that there are several ways that platforms might flexibly achieve this goal. For example, requiring proof of insurance would provide a form of security for any reasonably foreseeable damages to consumers that might flow from the use of the product. Rights holders could also be compensated in cases of infringement.

## 7. Clear Transactions Through Banks that Comply with U.S. Enforcement Requests

Many foreign sellers on third-party marketplaces do not have a financial nexus to the United States, making it difficult to obtain financial information and to subject all parts of the transaction to U.S. law enforcement efforts.

Platforms should close this loophole by encouraging all sellers to clear transactions only with banks and payment providers that comply with U.S. law enforcement requests for information and laws related to (relevant to) the financing of counterfeit activity.

## 8. Pre-Sale Identification of Third-Party Sellers

Stakeholders have, at times, reported that buyers have been surprised to discover upon completion of an online sales transaction, that the order will be fulfilled by an unknown third-party seller and *not* the platform itself. Without addressing the separate legal question of whether this comprises deceptive action *per se*, at least some buyers may have made different purchasing decisions if they

had known, prior to purchase, the identity of the third-party “storefront” owner, and/or the party ultimately responsible for fulfilling the transaction.

To increase transparency on this issue, platforms should significantly improve their pre-sale identification of third-party sellers so that buyers can make informed decisions, potentially factoring in the likelihood of being sold a counterfeit or IPR infringing merchandise. Platforms should implement additional measures to inform consumers, prior to the completion of a transaction, of the identity of storefront owners and/or those responsible for fulfilling a transaction, as well as any allegations of counterfeits being sold by a particular seller. On the converse, if a particular seller is a licensed reseller of the product, this information should also be provided.

Even if this information may be currently available, firm steps should be taken to ensure that this information is featured prominently in product listings. This will prompt greater consumer awareness and lead to more informed decision-making.

#### 9. Establish Marketplace Seller IDs

Platforms generally do not require a seller on a third-party marketplace to identify the underlying business entity, nor to link one seller profile to other profiles owned by that same business, or by related businesses and owners. In addition, the party that appears as the seller on the invoice and the business or profile that appears on the platform to be the seller, may not always be the same. This lack of transparency allows one business to have many different profiles that can appear unrelated. It also allows a business to create and dissolve profiles with greater ease, which can obfuscate the main mechanism that consumers use to judge seller credibility, namely reviews by other buyers.

Platforms should require sellers to provide the names of their underlying business or businesses (if applicable), as well as any other related seller profiles owned or controlled by that seller or that clear transactions through the same merchant account. Platforms can use this seller ID information in three helpful ways:

First, to communicate to the consumer a more holistic view of “who” is selling the goods, allowing the consumer to inspect, and consult reviews of, all related seller profiles to determine trustworthiness. Second, linking all related sellers together will assist rights holders in monitoring who is selling goods that they believe to be infringing. Third, the platform can use the connections to other seller profiles to better conduct its own internal risk assessment, and make risk mitigation decisions (e.g., requiring cash deposits or insurance) as appropriate based on the volume and sophistication of the seller.

#### 10. Clearly Identifiable Country of Origin Disclosures

Brick-and-mortar retail stores are required to have labels on their products that clearly identify the country or countries of origin. No such requirement applies to online e-commerce.